(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
28 juillet 2005 (28.07.2005)

PCT

(10) Numéro de publication internationale
WO 2005/069210 A1

(51) Classification internationale des brevets[7] :
G06K 19/077, H01L 23/58

(21) Numéro de la demande internationale :
PCT/FR2004/050756

(22) Date de dépôt international :
23 décembre 2004 (23.12.2004)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0351221 29 décembre 2003 (29.12.2003) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **COMMISSARIAT A L'ENERGIE ATOMIQUE** [FR/FR]; 31-33 rue de la Fédération, F-75752 PARIS 15ème (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **SAVRY, Olivier** [FR/FR]; 25, rue du Vercors, F-38000 GRENOBLE (FR). **BILLARD, Christophe** [FR/FR]; 844, rue de la République, F-38140 RENAGE (FR).

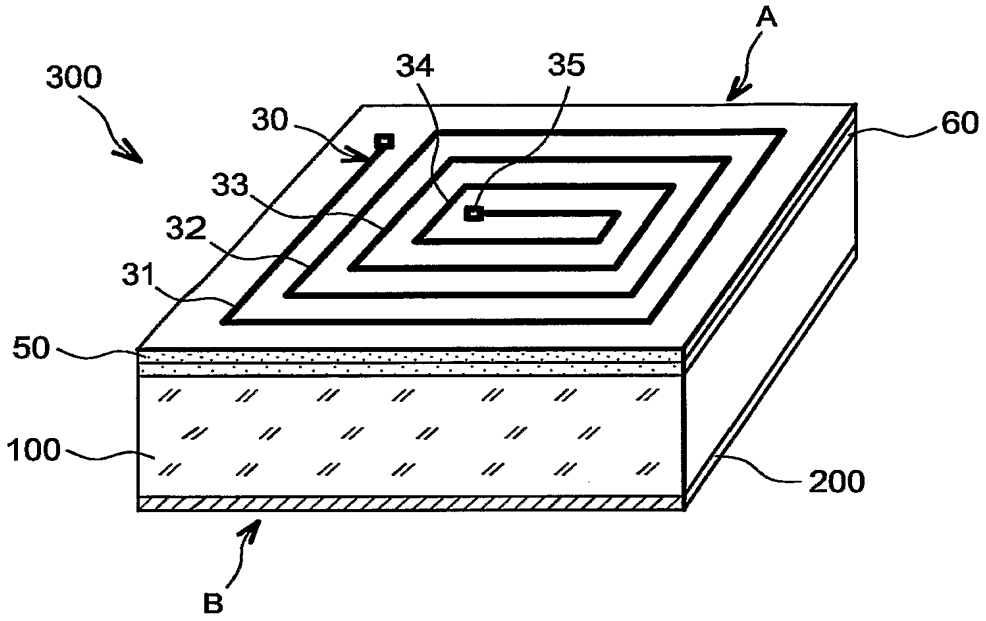
(74) Mandataires : **LEHU, Jean** etc.; Brevatome, 3, rue du Docteur Lancereaux, F-75008 Paris (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[Suite sur la page suivante]

(54) Title: PROTECTION FOR AN INTEGRATED CIRCUIT CHIP CONTAINING CONFIDENTIAL DATA

(54) Titre : PROTECTION D'UNE PUCE DE CIRCUIT INTEGRE CONTENANT DES DONNEES CONFIDENTIELLES



(57) Abstract: The invention relates to an integrated circuit chip (300) for holding or processing data on information for secure protection. According to the invention, a first side (A) of the chip has at least one first conductor element (30) and another side (B) of the chip has another conducting element (200).

(57) Abrégé : L'invention concerne une puce (300) de circuit intégré destiné à contenir ou traiter des données d'information à protéger de manière sécurisée. Selon l'invention, un premier côté (A) de la puce comporte au moins un premier élément conducteur (30) et un autre côté (B) de la puce comporte un autre élément conducteur (200).

WO 2005/069210 A1

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* **:** ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

PROTECTION D'UNE PUCE DE CIRCUIT INTEGRE CONTENANT DES DONNEES CONFIDENTIELLES

DESCRIPTION

DOMAINE TECHNIQUE ET ART ANTERIEUR

La présente invention concerne la protection des circuits intégrés électroniques et porte plus particulièrement sur des moyens pour empêcher l'accès à des contenus sensibles à la sécurité, tels que des données d'informations confidentielles, des codes de cryptage ou de décodage, des programmes ou des données secrètes, ou même simplement des données objet de propriété à protéger, stockées en mémoire de circuits intégrés.

L'invention s'adresse particulièrement à la sécurisation des circuits intégrés à mémoire, à microprocesseur ou à microcontrôleurs (y compris les circuits intégrés à application spécifique dits ASIC) qui sont utilisés par exemple, dans les domaines des cartes à puces, des transactions de paiement électronique, des distributeurs de billets, des dispositifs de porte-monnaie électronique, le domaine du cryptage/décodage de signaux audiovisuels de télévision à péage, le domaine des téléphones mobiles, le domaine des système d'accès sécurisés ou d'identification comme les cartes de santé et les dispositifs analogues.

Pour accéder aux données protégées dans les circuits intégrés, les personnes non autorisées, connues sous le nom de « pirates », disposent de

plusieurs méthodes d'investigation. Les pirates commencent généralement par désencapsuler le circuit intégré en enlevant le matériau du boîtier du composant 2, comme suggéré sur la figure 2A, pour accéder à la puce de substrat 20 du circuit intégré proprement dit.

Les éléments 21 du circuit intégré qui stockent, transmettent et traitent les données secrètes sont implantés sur la surface supérieure du substrat 20 qui est recouverte de plusieurs couches successives de revêtement, tels que des couches de passivation du substrat, de métallisation de circuiterie et d'isolation.

Les pirates cherchent à enlever les couches de revêtement par ablation mécanique, par attaque chimique, par dissolution acide, par découpage laser, par attaque de type communément appelé DFA (abréviation de « Differantial Fault Analysis ») pour accéder aux pistes du circuit et à la topographie du circuit électronique, de façon à dériver les signaux de données ou percer le fonctionnement du circuit.

Plusieurs méthodes peuvent permettre aux pirates d'accéder aux données. Ils peuvent utiliser des sondes de contacts microscopiques pour repiquer les signaux échangés sur les bus (éventuellement en perçant des trous), ou à l'aide de sondes électromagnétiques sans contact ou en utilisant un dispositif de microscopes optiques confocaux pour révéler le schéma électronique du circuit intégré, ou en utilisant une station de travail à faisceau d'ions focalisé (FIB) pour décaper très finement les matériaux de revêtement,

métaux ou isolants, et recomposer la structure du circuit (topographie) avec une très haute résolution.

Une autre méthode consiste à utiliser un dispositif perfectionné de microscope à balayage électronique (SEM), qui permet de révéler les potentiels électriques des signaux échangés dans les puces, la mesure étant faite sans contact au travers de la puce.

A l'heure actuelle, on connaît des dispositifs destinés à protéger la puce contre ces intrusions par la face avant.

Le document US-4 933 898 décrit une puce de circuit intégré sécurisé par une carapace de protection conductrice disposée sur la face avant de la puce, comme schématisé sur les figures 1A et 1B annexées ci-après.

La vue en coupe de la figure 1B montre que la structure du composant 1 de circuit intégré comporte des plans métallisés 13,15,17 formant des écrans aménagés dans des couches supérieures 12,14,16 déposées sur le substrat 10 du circuit intégré 1.

Selon l'enseignement du document US 4 933 898, ces écrans recouvrent des zones sensibles 17 correspondant aux circuits MP,BUS,MEM à transistors FT1,…,FT3 qui contiennent les données à protéger (mémoire MEM, bus de transmission BUS, unité de traitement MP, par exemple). Chaque écran 13, 15 ou 17 est relié, par l'intermédiaire de trous métallisés 11 (via) traversant les couches supérieures 12-14-16 aux circuits à transistors FT1,…,FT3 et conduit un signal d'alimentation VCC ou GND nécessaire au fonctionnement

ce ces circuits. Cette carapace métallique a pour fonction d'une part, d'empêcher une analyse au microscope à balayage électronique (SEM), aux rayons X ou par d'autres moyens électromagnétiques à travers la puce 1 et d'autre part, en cas d'intrusion ou d'ablation mécanique d'un tel écran conducteur 17, 15 ou 13, de provoquer une coupure d'alimentation des circuits à transistors détruisant automatiquement les données secrètes.

L'inconvénient d'un tel dispositif est que seule la face avant est protégée contre des intrusions ou des attaques destinées à percer la confidentialité des données sauvegardées. La face arrière 19,B reste accessible à une analyse ou à une attaque d'un pirate pour accéder aux données protégées.

Le document US-5 861 662 décrit un autre système de protection anti-piratage d'un circuit intégré 2, illustré sur les figures 2A et 2B annexées.

Des fils de liaison (en anglais, « wire bonds ») 23 s'étendent au dessus des circuits sécurisés 21 traitant les données à sauvegarder (tels qu'une unité de calcul CPU, un circuit périphérique DES de standard d'encryptage de données, une mémoire de type RAM, ROM ou autre). Les fils 23 sont noyés dans la masse du matériau d'encapsulation 28, constitué d'une couche d'époxy 28, qui recouvre les zones d'implantation de ces circuits électroniques sensibles 21. Les fils de liaison 23 transmettent les signaux nécessaires au fonctionnement de ces circuits actifs 21 et sont reliés audits circuits 21 par l'intermédiaire de plots P constitués par des trous métallisés 22,24

(via) traversant les couches de vitrification 25, de métallisation 26 et de passivation 27 qui recouvrent successivement le substrat semi-conducteur 20 et séparent la puce du matériau d'enrobage 28 à l'intérieur du boîtier du composant 2.

La couche de métallisation 26 intégrée dans les couches de protection 25 à 27 recouvrant le substrat 20 forme, là encore, un écran à l'analyse au microscope à balayage électronique (SEM).

La puce 20 du circuit intégré se présente alors incluse dans le matériau d'encapsulation qui forme une couche supérieure d'époxy 28 comportant le filet de fils de protection et une couche inférieure d'époxy 29 inerte. La puce 20 est finalement reportée dans le boîtier externe du composant 2 et reliée aux pattes de connexion (« pads/pins »).

L'inconvénient ici est encore que seule la face avant A, c'est-à-dire le côté supérieur de la puce 20, est protégée contre des intrusions ou attaques pirates.

Aucune protection n'est prévue en face arrière 29-B.

Les seules dispositions adoptées en général concernant la face arrière B des puces de circuit intégré contenant des données confidentielles consistent à envelopper totalement la puce dans un matériau d'encapsulation 29 difficile à enlever. Mais les pirates sont en mesure d'attaquer aisément ces matériaux d'encapsulation. En effet, les pirates reportent maintenant les attaques sur la face arrière suite aux dispositions de protection de la face avant

prises par les constructeurs de circuits intégrés, notamment pour les cartes à puce. Les méthodes utilisées par les pirates pour l'attaque de la face arrière sont classiquement des attaques DFA, découpe laser, analyse électromagnétique en général, etc….

La communication de R. Anderson et M. Kuhn, intitulée « Tamper resistant – a cautionary note », publiée dans le « second USENIX Workshop on Electronic Commerce Proceedings » (page 1 à 11) en novembre 1996, décrit la plupart des méthodes d'attaques pirates connues actuellement.

L'inconvénient des dispositifs connus est de ne disposer d'aucune protection en face arrière.

L'objet de l'invention est de réaliser des circuits intégrés remédiant aux inconvénients précédents.

Un objectif de l'invention est de fournir une protection de la face arrière des puces de circuit intégré dont la sécurité est sensible.

Un autre objectif de l'invention est d'améliorer en général la protection d'un circuit intégré contenant des données secrètes, aussi bien sur la face arrière que sur la face avant.

L'objectif en particulier est de protéger un circuit intégré contenant des données sensibles contre toutes sortes d'attaques pirates sur les deux faces opposées de la puce, tels que les attaques lasers, les inspections électromagnétiques sans contact, les analyses au microscope à balayage électronique (SEM), ou avec des microscopes confocaux, les attaques DFA, les intrusions par décapage mécanique

ou chimique, les intrusions par microsondes, les analyses chimiques (avec révélateurs cristallographiques ou ioniques), la résolution structurelle à l'aide d'un dispositif à faisceau d'ions focalisé (FIB), etc….

Un autre objectif est d'obtenir un circuit intégré disposant d'une protection complète des faces dont la mise en œuvre soit simple, en particulier n'impliquant pas la fabrication de via à travers toute l'épaisseur de la puce.

EXPOSÉ DE L'INVENTION

Ces objectifs sont atteints en prévoyant selon l'invention, qu'un circuit intégré contenant des informations sensibles dispose d'une protection complète comportant un premier élément conducteur disposé côté supérieur ou au niveau d'une première face, par exemple la face avant de la puce du circuit intégré et formant une inductance superficielle, associé avec un autre élément métallique ou conducteur en général, disposé côté inférieur ou au niveau d'une seconde face, par exemple la face arrière de la puce, cet autre élément superficiel modifiant le champ et/ou la valeur de l'inductance, de sorte que toute variation de l'inductance provoquée par une attaque et/ou une atteinte, et/ou une intrusion de l'élément inductif en face arrière ou une attaque (atteinte/intrusion) de l'inductance elle-même en face avant soit détectée par le circuit intégré, lequel dispose de moyens pour déclencher des contre-mesures, comme l'effacement des

informations codées ou des données sauvegardées en mémoire.

Le dispositif de protection selon l'invention peut être formé simplement d'une spirale ou d'un serpentin d'inductance métallisée, déposée sur ou dans un plan superficiel, côté supérieur de la puce et couplée avec un plan métallisé disposé sur ou sous la surface arrière côté inférieur de la puce, ce plan pouvant former par exemple un réflecteur électromagnétique.

Il est prévu que l'élément conducteur de l'inductance est relié aux pistes et aux transistors du circuit électronique, dont elle est séparée par une couche de passivation, par l'intermédiaire de trous métallisés (via) traversant cette passivation.

Par contre, l'élément conducteur de la face arrière étant couplé sans contact à l'inductance de la face avant, il n'est pas nécessaire de le relier au circuit intégré de la puce, et la face arrière ne comporte aucun via de connexion. En effet, l'invention permet avantageusement d'éviter d'aménager un trou métallisé (via) à travers l'épaisseur du substrat semi-conducteur, ce qui poserait un problème techniquement.

Ainsi, de façon avantageuse, la face arrière de la puce est protégée sans aménager de trou métallisé à travers la puce de substrat. Une métallisation pleine plaque de la face arrière est suffisante pour parachever la protection de la puce en face arrière.

L'invention met en oeuvre un dispositif électronique comprenant une puce de circuit intégré destiné à contenir, notamment stocker, mémoriser, transmettre ou traiter, des données d'information à protéger de manière sécurisée, comme des données secrètes, des données de cryptage ou de décodage, dans lequel un premier côté de la puce comporte au moins un premier élément conducteur et en ce qu'un autre côté de la puce comporte un autre élément conducteur.

Le premier élément conducteur et l'autre élément conducteur peuvent être couplés.

Selon une mise en oeuvre, le premier côté de la puce peut comporter, en outre, un deuxième élément conducteur disposé à proximité du premier élément conducteur.

Selon l'invention, le premier élément conducteur et/ou le deuxième élément conducteur peut comporter une inductance, tandis que l'autre élément conducteur peut former un plan de masse à faible résistance et/ou comporter une conductance.

Selon l'invention, le circuit électronique intégré sur ou dans la puce peut comporter des moyens d'excitation électromagnétique du premier élément conducteur.

Il peut être prévu aussi que le circuit électronique intégré comporte des moyens de mesure de l'inductance d'au moins un des éléments conducteurs.

Le circuit intégré peut comporter encore des moyens de détection d'un changement de valeur d'au moins un paramètre électrique du ou des éléments conducteurs, notamment un changement de valeur

d'inductance ou de résistance du premier et/ou du deuxième élément conducteur.

Et, il peut être prévu que le circuit intégré comporte des moyens pour effacer ou cesser de stocker les données d'information en cas de détection de changement de valeur de paramètre électrique.

Avantageusement, le premier élément conducteur et/ou le deuxième élément conducteur peut être relié au circuit électronique intégré de la puce par l'intermédiaire d'au moins et/ou au moins d'une connexion également appelée « via » traversant une ou des couches de revêtement recouvrant le premier côté de la puce, tandis que l'autre côté ne comporte pas de via ou de connexion.

Pour finir, les éléments conducteurs de la puce sont recouverts d'un matériau d'encapsulation.

L'invention peut être mise en œuvre notamment dans une carte à puce, comprenant au moins un tel dispositif électronique de puce de circuit intégré.

L'invention peut également s'appliquer à un dispositif de cryptage ou de décodage, comprenant un ou plusieurs de tels dispositifs électroniques de puce de circuit intégré.

BRÈVE DESCRIPTION DES DESSINS

D'autres objectifs, caractéristiques et avantages de l'invention apparaîtront à la lecture de la description détaillée ci-après, de modes de réalisation de l'invention, faite à titre d'exemple non limitatif, en regard des dessins annexés sur lesquels :

- les figures 1A et 1B représentent, vue de dessus et en coupe, une puce de circuit intégré avec une protection en face avant, selon l'état de la technique ;

- les figures 2A et 2B représentent, vue de dessus et en coupe, une puce de circuit intégré comportant des fils de protection en face avant, selon l'état de la technique ;

- les figures 3A et 3B représentent, en vue plongeante et en coupe, une puce de circuit intégré avec des éléments conducteurs de protection en face avant et en face arrière, selon l'invention ;

- la figure 4 représente une vue de dessus de l'implantation de deux éléments conducteurs en face avant d'une puce de circuit intégré selon l'invention ;

- la figure 5 représente une vue en coupe de niveaux d'interconnexion entre les éléments conducteurs en face avant et la puce de circuit intégré, selon l'invention ;

- les figures 6A et 6B représentent un mode de réalisation d'enroulement conducteur sur une puce de circuit intégré, selon l'invention ; et,

- les figures 7A et 7B représentent un autre mode de réalisation d'élément conducteur sur une puce de circuit intégré, selon l'invention.

EXPOSÉ DÉTAILLÉ DE MODES DE RÉALISATION DE L'INVENTION

Les figures 3A et 3B schématisent un premier mode de réalisation d'un circuit intégré sécurisé 300 qui illustre le principe de l'invention.

Sur les figures, la puce de circuit intégré 300 est représentée nue, sous une forme dépouillée, hors de tout matériau d'encapsulation ou d'enrobage et sans patte de connexion, éléments qui peuvent constituer les éléments extérieurs du boîtier d'un composant électronique achevé.

Le cœur du circuit intégré 300 est formé d'une puce de substrat 100 dans lequel sont implantés les éléments du circuit électronique, tels que les transistors, diodes, résistances, condensateurs etc…, qui ne sont pas représentés ici.

La puce 300 est constituée d'un petit morceau de matériau semi-conducteur généralement parallélépipédique et de dimensions miniatures (de l'ordre de quelques micromètres à plusieurs dizaines de millimètres, voire plus, typiquement entre une centaine de micromètres et plusieurs micromètres, généralement une fraction de micromètre ou quelques micromètres, par exemple : 0,25 micron ou 1,3 micron de côté pour 0,15 micron d'épaisseur environ).

Selon l'invention, la puce de circuit intégré 300 comporte un premier élément conducteur 30 disposé sur ou dans le côté supérieur de la puce 300 correspondant à la face avant A, par exemple sur une première couche 50 de passivation, pouvant elle-même reposer sur une deuxième couche 60 de passivation. La puce comporte d'autre part un autre élément conducteur 200 disposé en face arrière B, côté inférieur de la puce 300.

Dans cette configuration, la disposition des éléments conducteurs sur les faces opposées A et B

de la puce 300 permet d'obtenir un couplage, de nature inductive ou électromagnétique, entre le premier élément conducteur 30 et l'autre élément conducteur 200.

Selon le mode de réalisation de la figure 3A, le premier élément conducteur 30 comporte un enroulement spiral inducteur à plusieurs spires 31, 32,33,34 et forme en quelque sorte un bobinage de self ou une bobine d'inductance. Suivant le schéma 3A, l'autre élément conducteur 200 est formé d'un plan métallique déposé sur la surface arrière B de la puce 300. Sur la figure 3B seules 3 spires 31, 32, 33 sont représentées.

Dans la configuration de la figure 3A, l'autre élément conducteur 200 est déposé à faible distance du premier élément conducteur 30 et dans l'axe ou du moins auprès de l'axe A-B des spires de la bobine d'inductance formée par le premier élément 30, si bien que l'autre élément conducteur 200 se trouve géométriquement dans le champ du premier élément 30.

L'interposition de l'autre élément conducteur 200 dans le champ du bobinage d'inductance du premier élément conducteur 30 modifie la valeur d'inductance de ce premier élément 30.

Une telle disposition permet avantageusement de protéger la face arrière B du circuit intégré 300. Elle confère plusieurs niveaux de protection.

D'une part, l'élément conducteur 200 en face arrière offre une protection passive. La métallisation de la face arrière forme une barrière

mécanique et un écran aux ondes électromagnétiques et aux particules.

Ainsi, l'élément conducteur 200 en face arrière protège contre les intrusions mécaniques et empêche de disposer une sonde électromagnétique pour capter les signaux sans contact.

L'élément 200 forme, en outre, un écran contre les rayons X et contre un faisceau d'électrons d'un microscope à balayage électronique (SEM).

L'élément conducteur 200 en face arrière offre ainsi une protection passive contre les attaques de pirates cherchant à percer l'accès aux données secrètes par le biais de tels moyens de visualisation ou d'investigation.

L'invention permet d'autre part une protection active en cas de tentative d'escamoter totalement ou partiellement la métallisation 200 de la face arrière B.

En effet, puisque l'inductance du premier élément conducteur 30 est modifiée par l'interposition de l'autre élément conducteur 200 dans son champ, l'ablation de cet autre élément 200 aura pour conséquence de faire varier la valeur de l'inductance du premier élément 30.

Ainsi, suivant l'exemple de réalisation des figures 6A et 6B, en déposant une structure formée d'une couche de revêtement 60 en oxyde ou en dioxyde de silicium sur laquelle est implantée une piste 30 en cuivre de dix micromètres de largeur (10 µm) enroulée en forme de grecque ou de spirale carrée à quatre spires 31,32,33,34 et en déposant une métallisation 200

de plan de masse en aluminium de cinq micromètres d'épaisseur (5 µm) de l'autre côté B d'une puce 100 carrée de deux cent cinquante micromètres de côté (250 µm) et de cent cinquante micromètres d'épaisseur (150 µm) en substrat de silicium (semi-conducteur de résistivité de quinze ohms centimètres) on obtient une variation de valeur d'inductance de l'ordre de un dixième (environ 10 %) en cas d'ablation du plan métallisé 200 en face arrière B. La référence 61 désigne un via et la référence 62 une couche de métallisation.

La puce a une taille ou une surface sensiblement comprise entre 3x3 mm^2 et 5x5 mm^2.

Une amplitude telle que mentionnée ci-dessus est suffisante pour que le circuit électronique puisse détecter une intrusion et déclencher des mesures contre le piratage consistant par exemple à effacer les données confidentielles ou à bloquer leur accès en lecture.

Par suite, l'invention dispose de moyens de protection active consistant à mesurer, constamment ou par intermittence, la valeur d'inductance du premier élément conducteur 30 en face avant.

De façon avantageuse, l'invention permet de vérifier l'intégrité du dispositif de protection 200 en face arrière par l'intermédiaire du premier élément conducteur 30 en face avant, ceci à distance et sans contact avec l'élément conducteur 200 en face arrière.

L'invention permet encore de protéger la face avant A contre les attaques pirates grâce au premier élément 30 disposé côté supérieur A de la puce.

Une tentative d'ablation d'une partie ou de la totalité des couches de passivation 50, 60 recouvrant le substrat 100 et le circuit électronique intégré se soldera par l'ablation ou le court-circuit des spires du premier élément conducteur 30, donc par une détection de disparition ou de variation de l'inductance. D'autre part, une tentative d'intrusion consistant à insérer une microsonde pour repiquer les signaux échangés sur les pistes de connexion du circuit intégré 300, se soldera par la coupure ou le court-circuit des pistes 31, 32, 33, 34 de l'élément conducteur 30, ce qui modifie la valeur d'inductance ou de résistance, ou plus généralement l'impédance du premier élément conducteur 30.

En outre, selon un autre mode de réalisation de l'invention, il est prévu de perfectionner la protection en disposant un deuxième élément conducteur 40 à proximité du premier élément conducteur 30 en face avant A, à la surface ou à l'intérieur (sous la surface) du premier côté de la puce.

La figure 4 montre un schéma d'implantation de deux éléments conducteurs 30,40 côté supérieur d'une puce de circuit intégré, selon cet autre mode de réalisation de l'invention.

Sur l'exemple de réalisation de la figure 4, le premier et le deuxième éléments conducteurs 30,40 sont constitués de deux bobines d'inductances formées par deux enroulements de pistes métalliques disposées en spirale de manière alternée et imbriquée l'une dans l'autre.

Avantageusement, les deux enroulements 30 et 40 sont reliés en série par une jonction sous-jacente 39, tel qu'un 'pont' ou un passage conducteur (en anglais « underpass ») si bien que leurs inductances s'ajoutent.

Ainsi, toute tentative d'intrusion amenant la coupure d'une piste de self-inductance 32-36, 41-44 ou un court-circuit entre les deux éléments conducteurs 30 et 40, se traduit par une modification de la valeur d'inductance totale des éléments conducteurs. Il suffit donc de mesurer constamment ou par intervalles de temps (réguliers ou irréguliers) la valeur d'inductance de l'ensemble des éléments 30 et 40 en série entre les connexions 31 et 46, pour détecter une intrusion dans le circuit intégré.

Selon l'invention, le circuit intégré comporte donc des circuits électroniques internes constituant des moyens d'excitation électromagnétique du premier élément conducteur 30, des moyens pour mesurer l'inductance de l'ensemble conducteur 30/40, et des moyens pour détecter un changement de valeur de l'inductance.

En cas de détection de changement de valeur d'un paramètre électrique, signifiant une violation du dispositif de protection, le circuit intégré active des mesures de protection contre l'intrusion consistant par exemple, à effacer les données secrètes, à bloquer le fonctionnement du circuit ou à interdire une transmission de données, notamment en sortie.

Des moyens d'excitation de l'inductance peuvent être des moyens générateurs d'un courant sinusoïdal, appliqué à l'inductance.

On peut alors remesurer, au choix, une variation de phase ou d'amplitude de cette sinusoïde, entre la tension aux bornes et le courant injecté, et ce à l'aide de moyens de mesure de variation, respectivement de phase ou d'amplitude.

Il est également possible de mesurer la fréquence de résonance d'un circuit constitué de l'inductance couplée avec un, ou des, composants de type R et/ou C ayant des valeurs connues. Dans ce cas, des moyens de mesure de résonance, ou de mesure de fréquence, sont mis en œuvre.

Des moyens d'excitation de l'inductance peuvent également être des moyens pour générer un signal rectangulaire, attaquant un circuit constitué de l'inductance, en série ou en parallèle avec une résistance déterminée.

Il est alors possible de mesurer, avec des moyens appropriés, une variation de temps de montée, ou de temps de descente, du signal.

Dans tous les cas, le signal mesuré peut se présenter sous la forme d'une tension dépendante de l'inductance. On cherche alors à comparer cette tension, image de l'inductance, avec une tension mémorisée qui fait office de référence. Une telle mémorisation dans le circuit peut être faite, dans des moyens de mémorisation, de façon analogique (par exemple par stockage dans une capacité) ou numérique (la référence étant stockée dans une mémoire ROM au

format binaire, et convertie par un CNA en tension analogique).

La comparaison entre la mesure et la valeur stockée s'effectue alors à l'aide de moyens comparateurs de tension.

Si ces deux valeurs sont trop différentes, on peut appliquer des contre mesures, consistant par exemple à arrêter l'alimentation de la puce (par exemple par un transistor entre la masse et le VCC), ou effacer la mémoire (plusieurs techniques pouvant être envisagées selon le type de mémoire utilisée), ou bloquer un élément vital du microprocesseur (par exemple l'accès à la pile, ou au registre,…).

Comme illustré figure 5, il est prévu de relier les circuits électroniques internes de la puce 500 avec le premier élément conducteur 30 et, le cas échéant, avec le deuxième élément conducteur 40, de façon à appliquer un courant inductif dans la bobine d'inductance 30 afin d'obtenir une excitation électromagnétique et de façon à effectuer les mesures électriques aux bornes des éléments conducteurs 30 et 40.

La figure 5 représente une vue en coupe d'une réalisation d'une puce de circuit intégré 500 qui fait apparaître un mode de connexion entre les éléments conducteurs 30 et 40 disposés par-dessus les couches d'isolation/métallisation/passivation successives de la puce de circuit intégré (éléments conducteurs supra puce) et les circuits électroniques internes de la puce 500. Les circuits internes de la puce de circuit intégré (non illustré en détail) contiennent les moyens

d'excitation électromagnétique du premier élément conducteur 30, les moyens de mesure de paramètres électriques du premier et/ou du deuxième élément conducteur 30/40 ainsi qu'éventuellement les moyens de détection de changement de valeur de paramètre électrique.

De façon avantageuse, il est prévu de relier le premier élément conducteur 30 au circuit électronique interne d'excitation et de mesure de paramètre électrique, par l'intermédiaire d'au moins un via, c'est-à-dire d'un trou aménagé au travers des couches de passivation/isolation 50/60/80 et rempli d'un dépôt métallique pour ramener le contact électrique à la surface.

L'exemple schématique de la figure 5 montre ainsi que des transistors T de commande aptes à délivrer un signal commuté ou un signal alternatif d'excitation à la bobine d'inductance 30, peuvent être reliés aux plages de connexions d'extrémité 31 et 37 du premier élément conducteur 30 par l'intermédiaire de plusieurs niveaux successifs de métallisation 62-52, 68-58 et de via d'interconnexion 61-51, 69-57 aménagés dans l'épaisseur des couches de revêtement 50-60-80 déposées au dessus du substrat 100 du circuit intégré de la puce 500.

Initialement, le substrat comporte par exemple des zones de diffusion ou d'implantation ionique d'éléments dopants formant des canaux de transistors à effet de champ de type MOSFET séparés par des caissons d'isolation en oxyde de type FOX.

Chaque transistor T comporte des métallisations de contact de source S, de grille G et de drain D, tous ces éléments étant recouverts d'une couche de passivation 80.

Chaque borne de contact S,G,D est surmontée d'un via, c'est-à-dire d'un trou métallisé traversant l'épaisseur de la couche de passivation 80, pour ramener le contact à la surface de la passivation.

Une couche de métallisation 62-64-66-68 est déposée et gravée sur la couche de passivation 80 pour former des pistes métallisées, matérialisant la topographie du circuit électronique proprement dit, c'est-à-dire les chemins du circuit d'interconnexion entre les bornes de contact des transistors T et celles des autres éléments composant le circuit.

Ce niveau de pistes métallisées d'interconnexion 62-64-66-68 est recouvert d'une couche 60 de revêtement isolant supplémentaire pour isoler et protéger les pistes du circuit.

Selon le mode de réalisation de la figure 5, des vias 61,63,65,67,69 sont aménagés à travers cette couche 60 pour ramener le contact des bornes de commandes S,G,D en connexion avec les bornes 31 et 37 des éléments conducteurs 30 et 40.

Un autre étage comportant un niveau de pistes métallisées 52-58 recouvert d'une couche de revêtement 50 peut encore être prévu au-dessus de cette structure étagée 60/80 pour réaliser une ou des interconnexions entre les bornes 31-37 et 41-46 des bobines d'inductances formées par le premier et le deuxième éléments conducteurs 30 et 40.

Comme schématisé figure 4, une telle disposition permet avantageusement de relier en série l'enroulement spiral du premier élément conducteur 30 avec l'enroulement spiral du deuxième élément conducteur 40, par l'intermédiaire d'une interconnexion 39 ou d'une jonction sous-jacente aménagée à l'intérieur de la couche 50 sur laquelle les pistes métalliques 31 à 37 et 41 à 46 des éléments conducteurs 30 et 40, sont elles même déposées.

Une telle interconnexion (en anglais « underpass ») comportant au moins un premier via 57 (69), une piste conductrice sous-jacente 39 (ou 58-69-68-...-62-61-52) et au moins un deuxième via 51 (61), permet de relier en série l'extrémité finale 37 du premier enroulement conducteur 30 à l'extrémité initiale 41 de l'autre enroulement conducteur 40. Ainsi on peut avantageusement relier en série les deux enroulements 30 et 40 imbriqués l'un dans l'autre sans inverser le sens de rotation du courant d'induction.

De tels vias et niveaux d'interconnexion permettent d'autre part de relier les bornes 31,41,37,46 des éléments conducteurs au circuit électronique interne de la puce, en particulier aux bornes des moyens d'excitation et des moyens de mesure de paramètres électriques.

Selon le processus de réalisation prévu par l'invention, le premier élément conducteur et/ou le deuxième élément conducteur sont implantés par dépôt de métallisation et gravure sur le premier côté de la puce, le dépôt des métallisations du premier et/ou du deuxième élément conducteur étant précédé par des

étapes de dépôt de couches de passivation, de métallisation et de gravure pour former au moins un niveau conducteur d'interconnexion intermédiaire entre le circuit électronique intégré et le ou les éléments conducteurs.

Le processus de réalisation prévoit encore que l'autre élément conducteur est formé par dépôt de métallisation sur l'autre côté de la puce.

Les figures 7A et 7B montrent un autre mode de réalisation permettant de supprimer une couche et un niveau d'interconnexion (« underpass ») entre les bornes du ou des éléments conducteurs 50 implantés côté supérieur en face avant, et d'éviter d'aménager un via d'interconnexion à ce niveau.

Selon le mode de réalisation de la figure 7A, le premier élément conducteur 70 est formé par un serpentin 71 à 74 comportant au moins un méandre 72, 73, constitué de tronçons de pistes métalliques sensiblement parallèles ici et interconnectés en alternance, suivant un chemin analogue au trajet d'aller-retour de navette d'un fil de trame.

Les méandres 72 et 73 du serpentin produisent un champ de nature inductive ou électromagnétique dans l'axe A-B transversal au plan du serpentin 70, champ dans lequel vient s'interposer l'autre élément conducteur 200 de l'autre face B de la puce, ce qui modifie la valeur d'inductance du serpentin du premier élément 70, selon le principe de l'invention.

Suivant l'exemple de réalisation des figures 7A et 7B, en implantant une telle piste

métallique en serpentin 70 en aluminium de cinq micromètres d'épaisseur (5 µm) pour former le premier élément conducteur sur une puce 100 de substrat (ou sur une couche 80 de passivation la recouvrant) de un et demi micromètres carrés (1300 µm x 1100 µm) ayant la même structure sous-jacente que dans l'exemple précédent, on obtient une variation d'inductance d'environ un quart (25 %) en cas d'ablation du plan de masse arrière 200.

De façon avantageuse plus la surface de la puce 700 occupé par l'enroulement ou les ondulations du premier élément conducteur et l'autre élément conducteur est importante, plus la variation d'inductance est marquée.

Les connexions permettant d'amener le courant d'excitation aux bornes 71 et 74 du serpentin du premier élément conducteur 70 et de mesurer les paramètres électriques de ce serpentin d'inductance 70 peuvent être réalisées à travers une ou deux couches d'isolation/passivation 80 par l'intermédiaire de via ramenant les bornes de contact S, G, D des transistors T et autres éléments composant le circuit électronique interne de la puce à la surface.

L'avantage de l'invention est que l'autre élément conducteur 200, disposé côté inférieur du substrat 100 pour protéger la face arrière contre des intrusions ou des attaques pirates, ne nécessite pas d'être relié au circuit électronique interne de la puce.

De façon avantageuse, le couplage inductif ou électromagnétique entre le premier élément, qui

protège la face avant, et l'autre élément conducteur, qui protège la face arrière, s'effectue à distance sans contact, ce qui permet de s'affranchir du problème de connexion entre le circuit électronique implanté en surface supérieure du substrat 100 et le côté inférieur de la puce correspondant à la face arrière B.

Ainsi, la puce ne comporte pas de via aménagé côté inférieur en face arrière. Aucun via ne traverse le substrat semi-conducteur 100 grâce à l'invention.

Selon le principe exposé précédemment, la disposition d'un premier élément conducteur 30 ou 70 en forme de bobinage d'inductance en face avant A, côté supérieur de la puce, et d'un autre élément conducteur 200 formé d'un plan métallisé en face arrière de l'autre côté du substrat 100, permet d'obtenir un couplage inductif ou électromagnétique entre les éléments conducteurs des faces opposées A et B.

A ce titre, diverses formes et variantes de réalisation peuvent être envisagées pour constituer les éléments conducteurs des deux faces du circuit intégré selon l'invention.

Dans les modes de réalisation exposés précédemment, l'élément conducteur côté inférieur est formé par un plan métallisé. Une telle surface métallisée permet avantageusement de former une masse métallique dans le champ géométrique, et plus précisément dans l'espace ou se propage le champ inductif ou le champ électromagnétique généré par l'inductance du premier élément conducteur.

Ainsi, l'autre élément conducteur forme un plan de masse ou une surface équipotentielle qui s'interpose dans le champ du premier élément conducteur.

De façon avantageuse, un tel plan de masse présente une résistance la plus réduite possible ou une conductance maximale ou du moins particulièrement élevée.

D'après une proposition avancée pour expliquer le phénomène à la base de l'invention, l'excitation de la self-inductance du premier élément conducteur 30 ou 70 induit un champ électromagnétique B qui fait apparaître un fort courant dans le plan de masse faiblement résistant formé par l'autre élément conducteur 200, lequel s'oppose à ce champ, ce qui revient à diminuer la valeur d'inductance du premier élément conducteur 30 ou 70.

Selon une autre forme de réalisation, le premier élément conducteur 10 et par extension, le deuxième élément conducteur 20, peuvent être constitués simplement d'une boucle de circuit s'étendant à la surface ou dans un plan sous la surface supérieure de la puce.

De façon générale, le premier élément conducteur 10, ainsi que le deuxième élément conducteur 20 peut être formé par une seule ou plusieurs pistes conductrices, de préférence métalliques et longilignes, s'étendant à la surface ou dans un plan inclus sous la surface du boîtier de la puce. Cette ou ces pistes peuvent être connectés à une seule de leurs extrémités pour recevoir le signal d'excitation.

Ainsi, selon une autre alternative, le premier élément conducteur et/ou le deuxième élément conducteur peut comporter plusieurs tronçons de pistes disposés de manière sensiblement parallèles et interconnectés bout à bout (cas du serpentin) ou par une seule extrémité en forme de peigne.

Le premier élément conducteur et le deuxième élément conducteur peuvent ainsi avoir des motifs alternés, entremêlés ou entrelacés.

L'autre élément conducteur en face arrière peut également prendre diverses formes pour réaliser la fonction de réflecteur d'antenne électromagnétique, la fonction d'écran et/ou de plan de masse.

L'élément conducteur en face arrière peut ainsi avoir le même motif ou une forme analogue au premier élément conducteur qui constitue l'antenne émettrice sur la première face.

Pour constituer un bon réflecteur, l'élément conducteur en face arrière a de préférence une bonne conductivité ou une faible résistance, comme un plan de masse.

Cet élément conducteur arrière peut être formé d'une armature conductrice, ou d'un enroulement spiral court-circuité, ou d'un serpentin court-circuité, ou d'une boucle de circuit court-circuitée, ou d'une seule piste conductrice ou de plusieurs pistes métalliques parallèles interconnectées.

Selon d'autres formes de réalisation, l'élément conducteur 10 de la face arrière est formé par un motif de maillage conducteur.

L'élément conducteur 10 de la face arrière peut ainsi comporter un réseau de mailles métalliques à maille circulaire ou polygonale, notamment hexagonale ou carrée.

En particulier, l'élément 10 en face arrière, peut être une grille métallique, notamment un réseau de grille en aluminium déposé sur la face arrière du substrat. Le nombre de mailles du réseau peut varier d'une seule maille (une boucle conductrice court-circuitée) à un nombre quelconque de mailles. Plus le nombre de mailles est grand, plus le maillage est serré et constitue une barrière de protection d'efficacité renforcée à l'intrusion d'une sonde ou à l'analyse aux rayons X ou au microscope à balayage électronique.

Par suite, d'autres formes, variantes et modes de réalisation pourront être mis en œuvre par l'homme de métier, sans sortir du cadre de la présente invention.

REVENDICATIONS

1. Dispositif électronique comportant une puce (300) de circuit intégré destiné à contenir ou traiter des données d'information à protéger de manière sécurisée, un premier côté (A) de la puce comportant au moins un premier élément conducteur (30), et un autre côté (B) de la puce comportant un autre élément conducteur (200), le premier élément conducteur (30) et l'autre élément conducteur (200) étant couplés.

2. Dispositif selon la revendication 1, caractérisé en ce que le premier côté (A) de la puce comporte, en outre, un deuxième élément conducteur (40) disposé à proximité du premier élément conducteur (30) et/ou relié en série (39) avec le premier élément conducteur (30).

3. Dispositif selon la revendications 2, caractérisé en ce que le premier élément conducteur (30) et le deuxième élément conducteur (40) comportent des motifs alternés entremêlés, enroulés ou entrelacés.

4. Dispositif selon l'une des revendications 1 à 3, caractérisé en ce que le premier élément conducteur (30) présente une armature émettrice.

5. Dispositif selon l'une des revendications 1 à 4, caractérisé en ce que le premier élément conducteur (30) et/ou le deuxième élément conducteur (40) comporte une inductance.

6. Dispositif selon l'une des revendications 1 à 5, caractérisé en ce que l'autre élément conducteur (200) comporte une conductance ou une faible résistance de plan de masse.

7. Dispositif selon l'une des revendications 1 à 6, caractérisé en ce qu'il comporte des moyens d'excitation électromagnétique du premier élément conducteur.

8. Dispositif selon l'une des revendications 1 à 7, caractérisé en ce que le circuit électronique intégré comporte des moyens de mesure de l'inductance d'au moins un des éléments conducteurs et/ou de détection de variation de l'inductance.

9. Dispositif selon la revendication 8, caractérisé en ce qu'il comporte des moyens pour effacer ou cesser de stocker les données d'information en cas de détection de changement de valeur de l'inductance.

10. Dispositif selon l'une des revendications 1 à 9, caractérisé en ce que le premier élément conducteur (30) et/ou le deuxième élément conducteur (40) est relié au circuit électronique intégré (T) à l'intérieur de la puce (100,500), tandis que l'autre élément conducteur (200) n'est pas relié.

11. Dispositif selon l'une des revendications 1 à 10, caractérisé en ce que la puce (500) comporte des couches supérieures de revêtement (50,60,80) comprenant au moins un niveau (52-62,58-68) métallique ou conducteur permettant de relier le premier élément conducteur (30) avec le circuit électronique intégré (T,100) et/ou avec le deuxième élément conducteur (40).

12. Dispositif selon l'une des revendications 1 à 11, caractérisé en ce que le premier et/ou le deuxième élément conducteur (30/40) forme une boucle de circuit.

13. Dispositif selon l'une des revendications 1 à 12, caractérisé en ce que l'autre élément conducteur (200) forme un plan de masse ou une équipotentielle.

14. Dispositif selon l'une des revendications 1 à 13, caractérisé en ce que le premier et/ou le deuxième élément conducteur (30/40) comporte au moins une piste métallique longiligne (32/42).

15. Dispositif selon l'une des revendications 1 à 14, caractérisé en ce que le premier et/ou le deuxième élément conducteur (30/40) comporte plusieurs tronçons interconnectés (32,33,34/42,43,44) disposés de manière sensiblement concentrique, de façon à former une grecque ou une spirale polygonale ou à former une spirale sensiblement circulaire.

16. Dispositif selon l'une des revendications 1 à 15, caractérisé en ce que le premier élément et/ou le deuxième élément conducteur (70) comporte plusieurs tronçons interconnectés (71,72,73,74) disposés de manière sensiblement parallèles de façon à former au moins un méandre ou un serpentin.

17. Dispositif selon l'une des revendications 1 à 16, caractérisé en ce que l'autre élément (200) comporte un plan ou une portion de surface métallisée ou un réseau de mailles conductrices, notamment un réseau à mailles sensiblement circulaires, carrées, hexagonales ou polygonales, ou une grille.

18. Dispositif selon l'une des revendications 1 à 17, caractérisé en ce que chaque élément conducteur (30,40,70,200) est inscrit dans un plan sensiblement parallèle à la surface de côté (A,B) de la puce.

19. Dispositif selon l'une des revendications 1 à 18, caractérisé en ce que les éléments conducteurs (30,40,70,200) de la puce sont recouverts d'un matériau d'encapsulation.

20. Carte à puce, caractérisée en ce qu'elle comprend au moins un dispositif électronique selon l'une des revendications 1 à 19.

21. Dispositif de cryptage ou de décodage caractérisé en ce qu'il comprend un ou plusieurs dispositifs électroniques selon l'une des revendications 1 à 19.

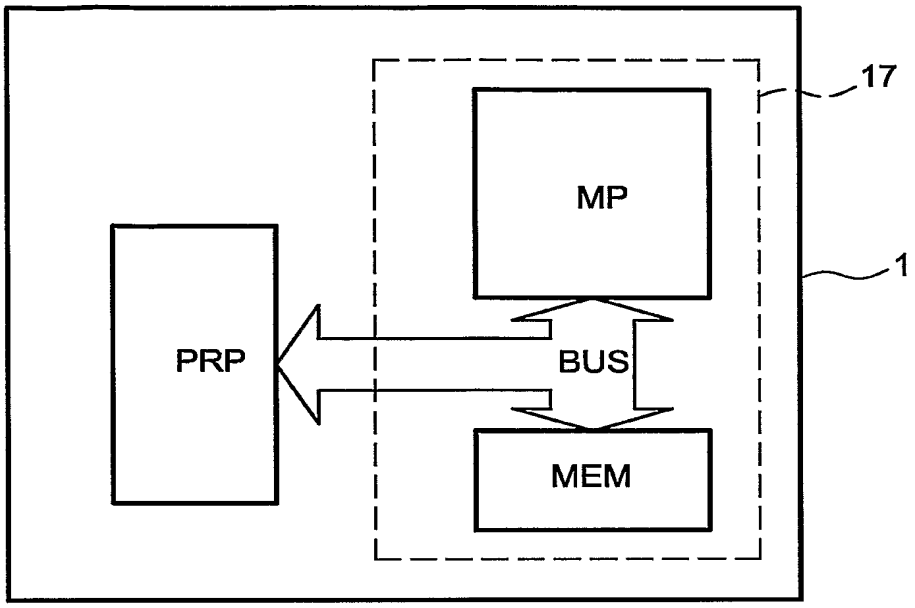

17
MP
1
PRP
BUS
MEM

FIG. 1A

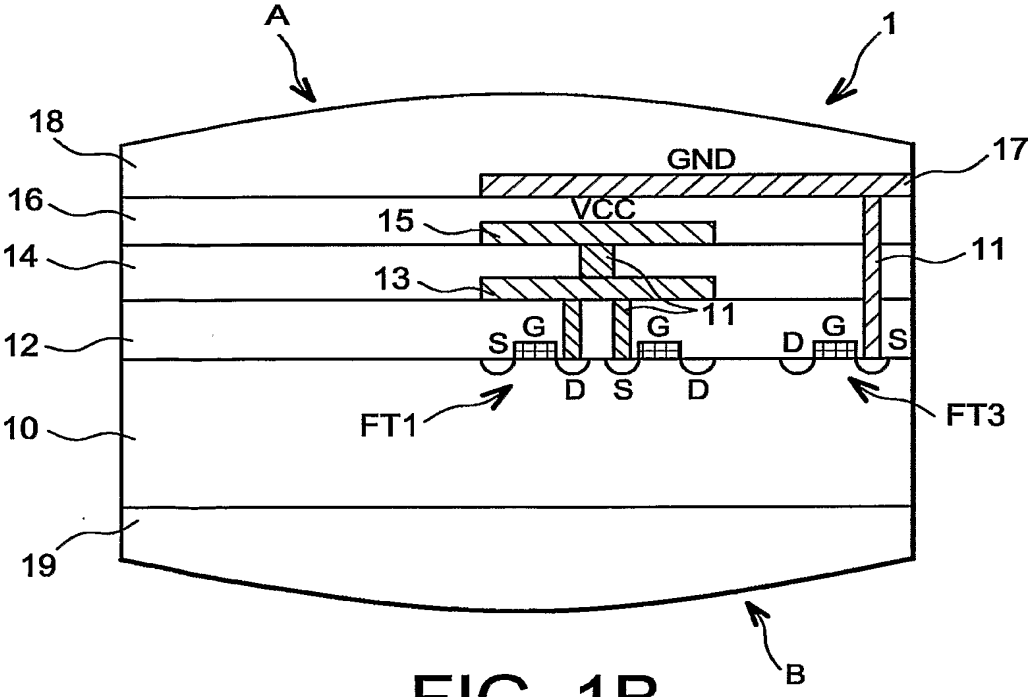

A
1
18
GND
17
16
VCC
15
14
11
13
11
12
S
G
G
D
G
S
D
S
D
FT1
FT3
10
19
B

FIG. 1B

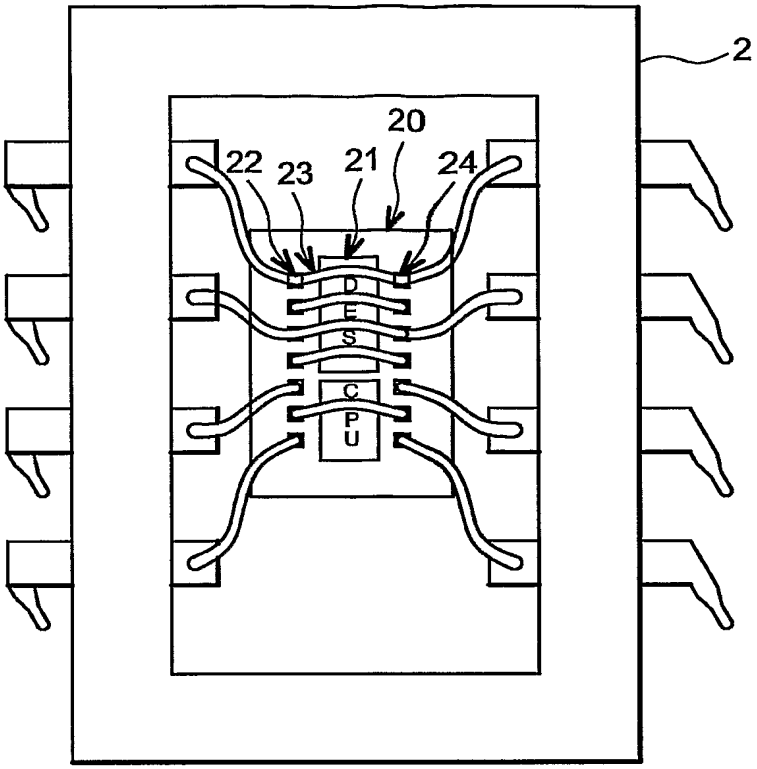


FIG. 2A

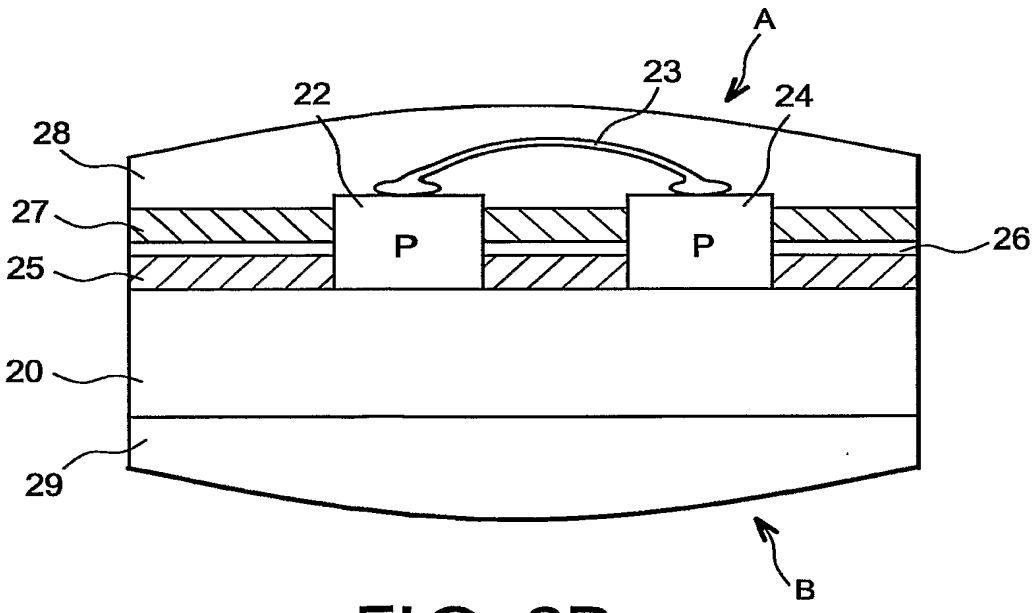


FIG. 2B

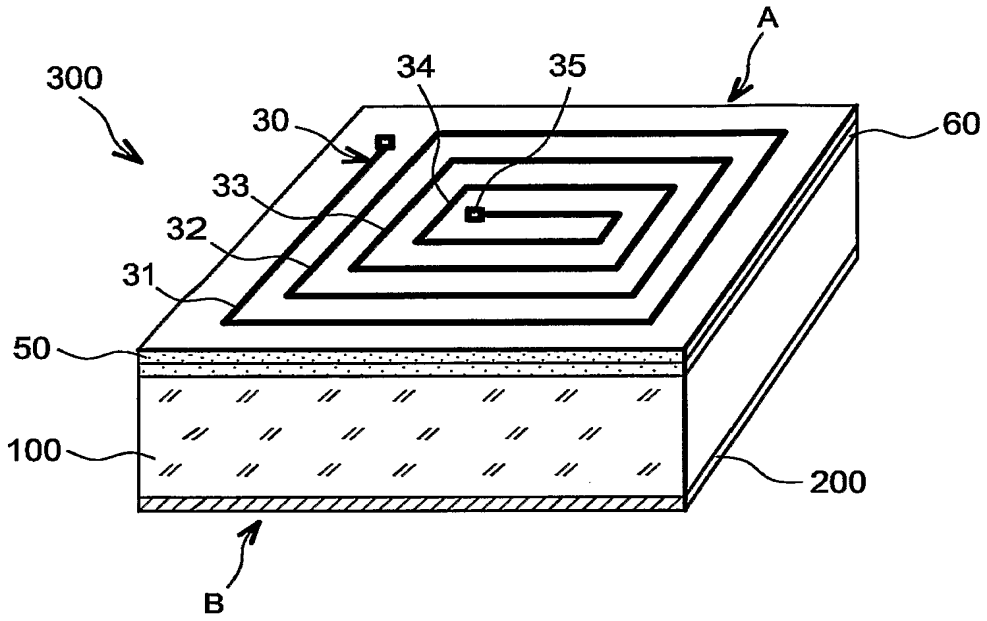

A
300
34
35
30
60
33
32
31
50
100
200
B

FIG. 3A

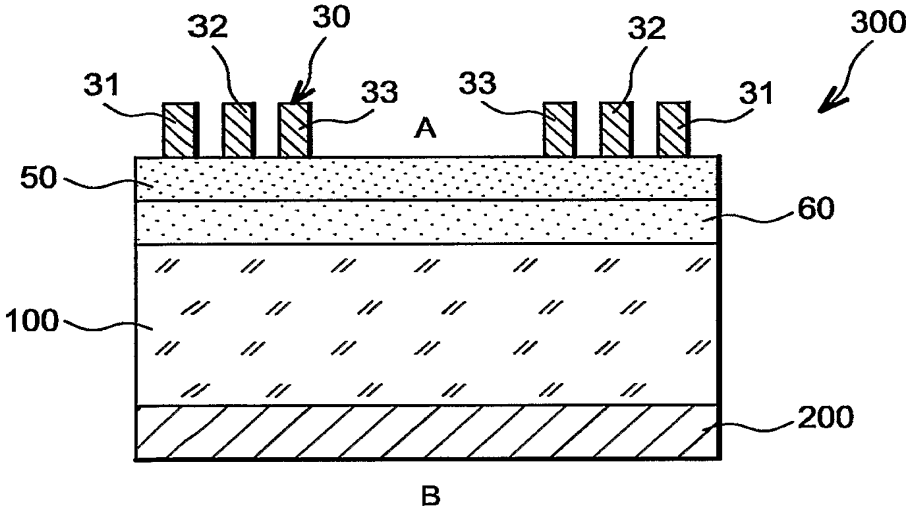

32
30
32
300
31
33
33
31
A
50
60
100
200
B

FIG. 3B

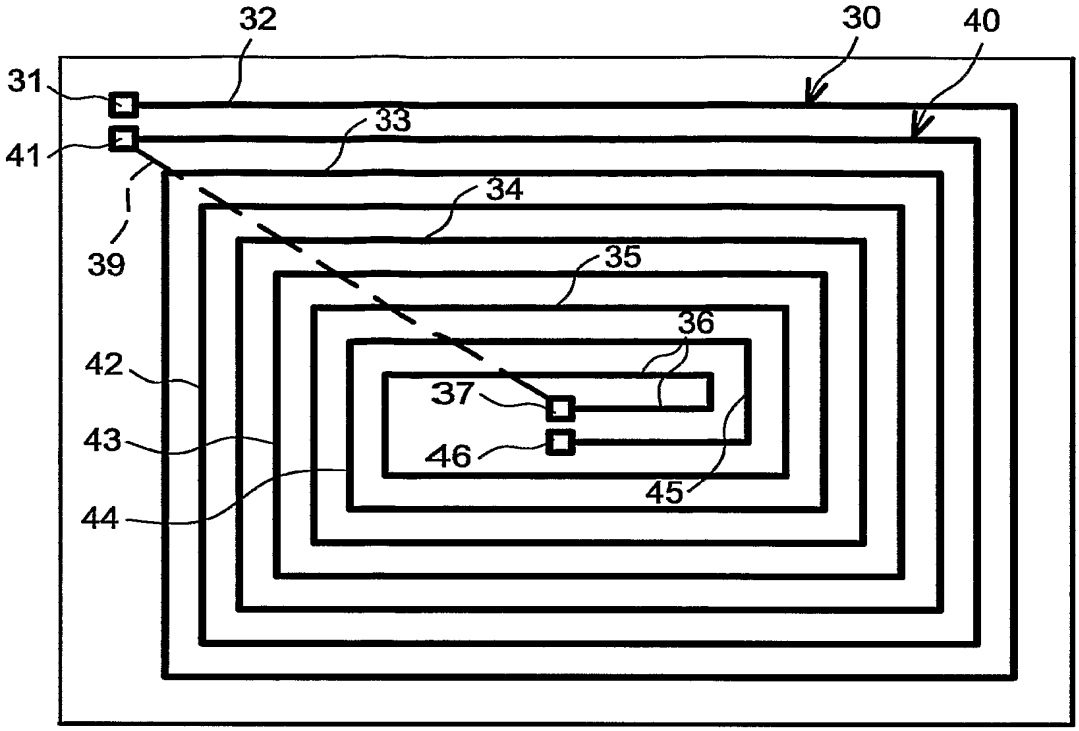

32
30
40
31
33
41
34
39
35
36
42
37
43
46
45
44

FIG. 4

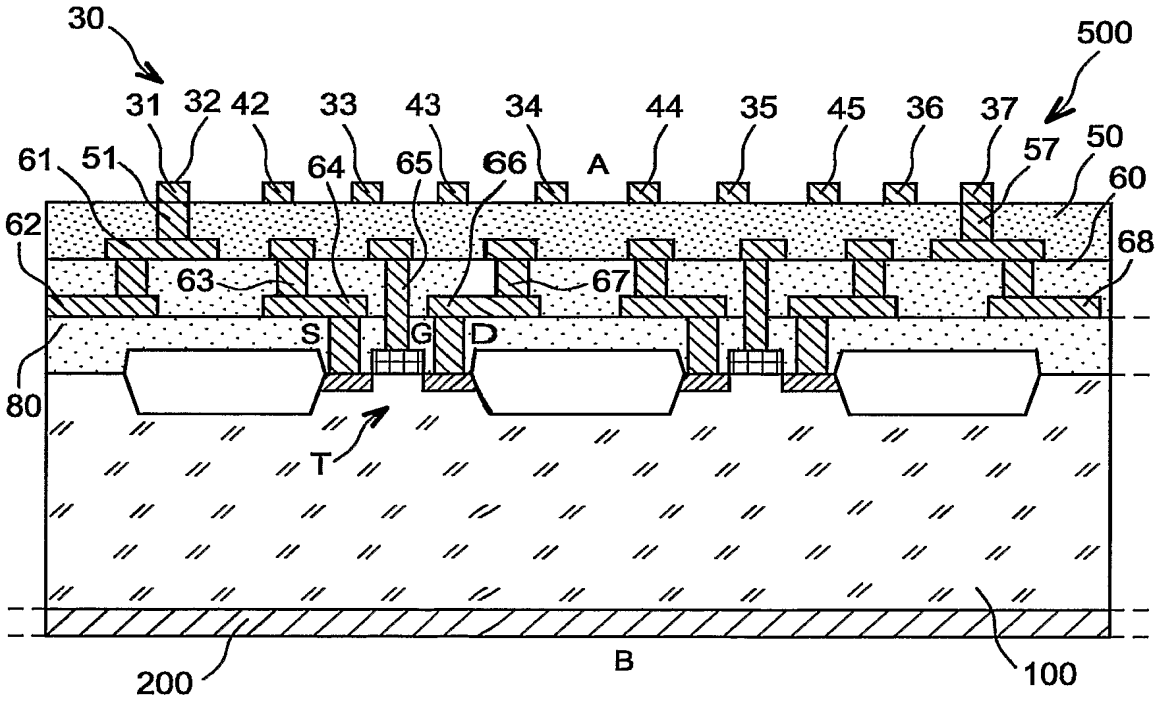

30
500
31
32
42
33
43
34
44
35
45
36
37
57
50
61
51
64
65
66
A
60
62
68
63
67
S
G
D
80
T
200
B
100

FIG. 5

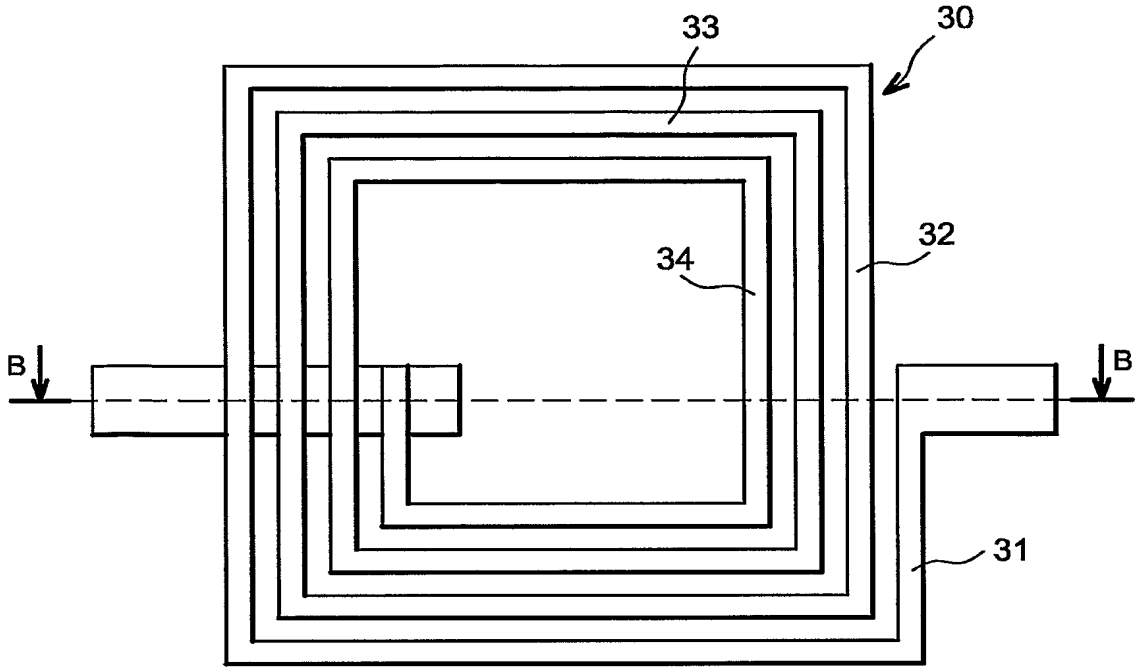


FIG. 6A

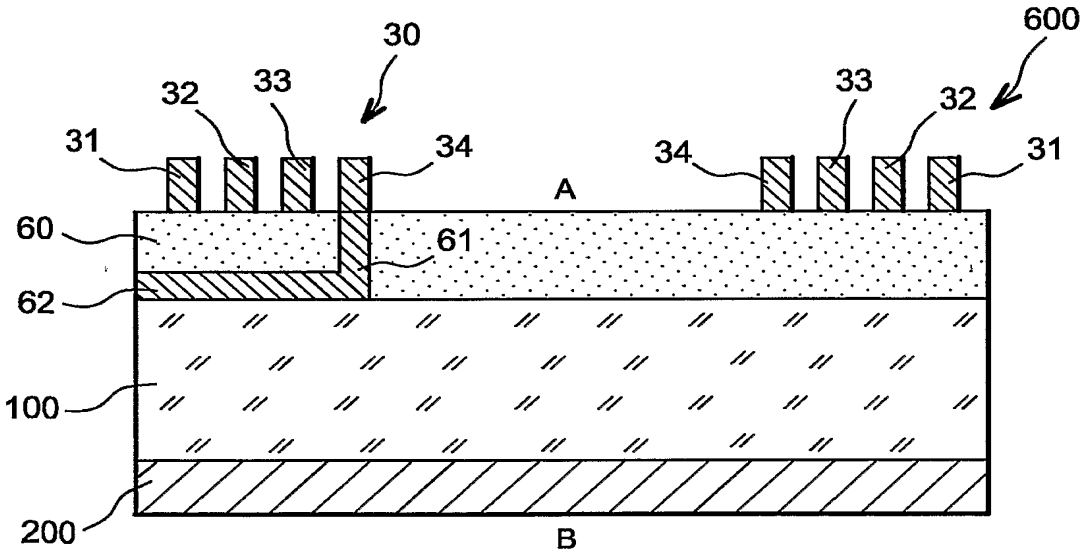
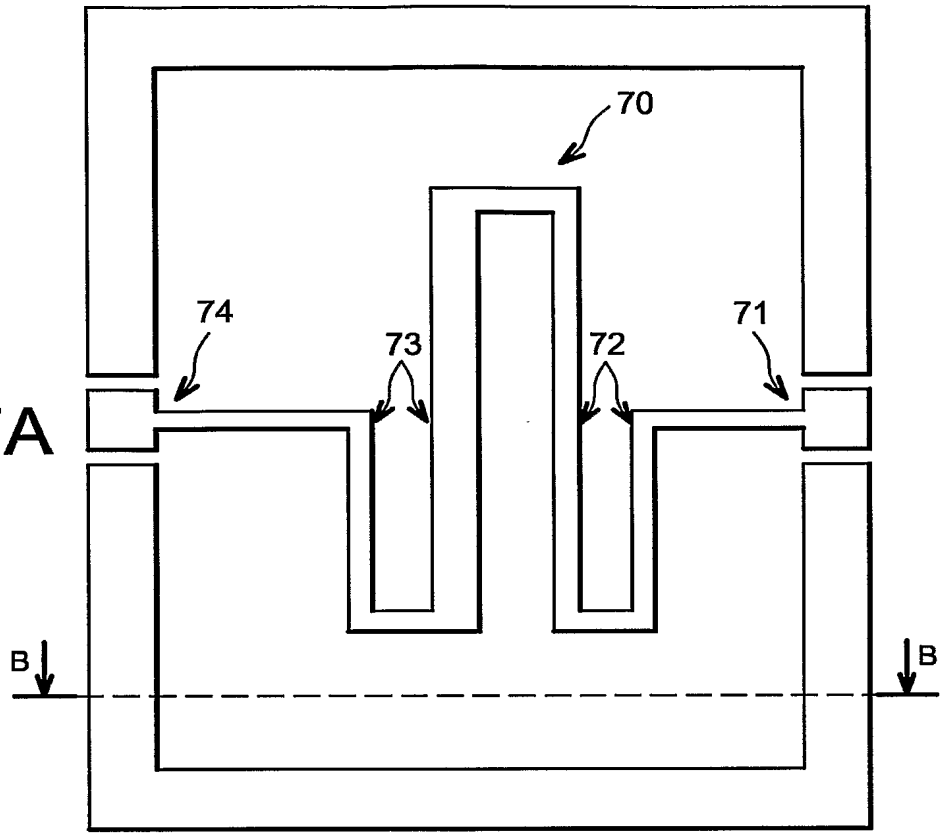


FIG. 6B

FIG. 7A



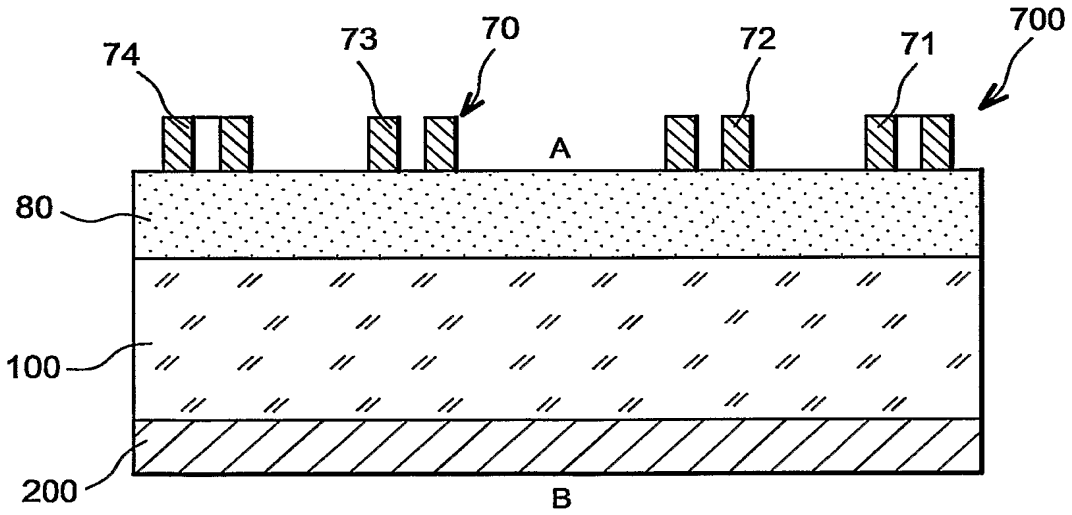


FIG. 7B

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR2004/050756

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K19/077 H01L23/58

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06K H01L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/008428 A1 (WEGERTSEDER DOMINIK ET AL) 24 January 2002 (2002-01-24)	1,2,4-7, 11-16, 18-21
Y	*the whole document*	3,16,17
Y	DE 197 38 990 A (SIEMENS AG) 11 March 1999 (1999-03-11) column 7, line 17 - column 8, line 55; figures 5,6	3,16,17
Y	EP 0 874 401 A (NIPPON ELECTRIC CO) 28 October 1998 (1998-10-28) column 3, line 12 - column 5, line 43; figures 1A,3A,3B	3,16,17
Y	US 6 246 970 B1 (WALMSLEY SIMON ROBERT ET AL) 12 June 2001 (2001-06-12) column 6, line 34 - line 57; figure 4	3,16,17

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 May 2005	10/05/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Schmidt, R

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR2004/050756

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4 933 898 A (KNOWLES RICHARD M ET AL) 12 June 1990 (1990-06-12) cited in the application the whole document	
A	US 5 861 662 A (CANDELORE BRANT) 19 January 1999 (1999-01-19) cited in the application the whole document	
A	KOEMMERLING O ET AL: "DESIGN PRINCIPLES FOR TAMPER-RESISTANT SMARTCARD PROCESSORS" USENIX WORKSHOP ON SMARTCARD TECHNOLOGY, XX, XX, 10 May 1999 (1999-05-10), pages 9-20, XP009010824 cited in the application the whole document	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR2004/050756

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002008428 A1	24-01-2002	DE 50004245 D1	04-12-2003
		WO 0045332 A1	03-08-2000
		EP 1149358 A1	31-10-2001
		JP 2002536727 T	29-10-2002
DE 19738990 A	11-03-1999	DE 19738990 A1	11-03-1999
EP 0874401 A	28-10-1998	JP 3037191 B2	24-04-2000
		JP 10294444 A	04-11-1998
		CN 1201259 A ,C	09-12-1998
		EP 0874401 A2	28-10-1998
		US 5986284 A	16-11-1999
US 6246970 B1	12-06-2001	NONE	
US 4933898 A	12-06-1990	AU 617026 B2	14-11-1991
		AU 4766990 A	19-07-1990
		CA 2007469 A1	12-07-1990
		DE 69033241 D1	16-09-1999
		DE 69033241 T2	03-02-2000
		DE 69034125 D1	05-02-2004
		DE 69034125 T2	18-11-2004
		DK 378306 T3	13-03-2000
		DK 920057 T3	10-05-2004
		EP 0378306 A2	18-07-1990
		EP 0920057 A2	02-06-1999
		ES 2134188 T3	01-10-1999
		ES 2214760 T3	16-09-2004
		IE 62793 B1	08-03-1995
		JP 2057246 C	23-05-1996
		JP 2232960 A	14-09-1990
		JP 7087237 B	20-09-1995
		KR 180521 B1	15-04-1999
		NO 900114 A	13-07-1990
		NO 975981 A	19-12-1997
US 5861662 A	19-01-1999	CA 2230065 A1	24-08-1998
		CN 1200570 A	02-12-1998
		EP 0860882 A2	26-08-1998
		JP 10294325 A	04-11-1998
		TW 388942 B	01-05-2000

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR2004/050756

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06K19/077 H01L23/58

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06K H01L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2002/008428 A1 (WEGERTSEDER DOMINIK ET AL) 24 janvier 2002 (2002-01-24)	1,2,4-7, 11-16, 18-21
Y	le document en entier	3,16,17
Y	DE 197 38 990 A (SIEMENS AG) 11 mars 1999 (1999-03-11) colonne 7, ligne 17 - colonne 8, ligne 55; figures 5,6	3,16,17
Y	EP 0 874 401 A (NIPPON ELECTRIC CO) 28 octobre 1998 (1998-10-28) colonne 3, ligne 12 - colonne 5, ligne 43; figures 1A,3A,3B	3,16,17
Y	US 6 246 970 B1 (WALMSLEY SIMON ROBERT ET AL) 12 juin 2001 (2001-06-12) colonne 6, ligne 34 - ligne 57; figure 4	3,16,17

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
2 mai 2005	10/05/2005

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Schmidt, R

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR2004/050756

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 4 933 898 A (KNOWLES RICHARD M ET AL) 12 juin 1990 (1990-06-12) cité dans la demande le document en entier	
A	US 5 861 662 A (CANDELORE BRANT) 19 janvier 1999 (1999-01-19) cité dans la demande le document en entier	
A	KOEMMERLING O ET AL: "DESIGN PRINCIPLES FOR TAMPER-RESISTANT SMARTCARD PROCESSORS" USENIX WORKSHOP ON SMARTCARD TECHNOLOGY, XX, XX, 10 mai 1999 (1999-05-10), pages 9-20, XP009010824 cité dans la demande le document en entier	

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR2004/050756

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2002008428 A1	24-01-2002	DE 50004245 D1	04-12-2003
		WO 0045332 A1	03-08-2000
		EP 1149358 A1	31-10-2001
		JP 2002536727 T	29-10-2002
DE 19738990 A	11-03-1999	DE 19738990 A1	11-03-1999
EP 0874401 A	28-10-1998	JP 3037191 B2	24-04-2000
		JP 10294444 A	04-11-1998
		CN 1201259 A ,C	09-12-1998
		EP 0874401 A2	28-10-1998
		US 5986284 A	16-11-1999
US 6246970 B1	12-06-2001	AUCUN	
US 4933898 A	12-06-1990	AU 617026 B2	14-11-1991
		AU 4766990 A	19-07-1990
		CA 2007469 A1	12-07-1990
		DE 69033241 D1	16-09-1999
		DE 69033241 T2	03-02-2000
		DE 69034125 D1	05-02-2004
		DE 69034125 T2	18-11-2004
		DK 378306 T3	13-03-2000
		DK 920057 T3	10-05-2004
		EP 0378306 A2	18-07-1990
		EP 0920057 A2	02-06-1999
		ES 2134188 T3	01-10-1999
		ES 2214760 T3	16-09-2004
		IE 62793 B1	08-03-1995
		JP 2057246 C	23-05-1996
		JP 2232960 A	14-09-1990
		JP 7087237 B	20-09-1995
		KR 180521 B1	15-04-1999
		NO 900114 A	13-07-1990
		NO 975981 A	19-12-1997
US 5861662 A	19-01-1999	CA 2230065 A1	24-08-1998
		CN 1200570 A	02-12-1998
		EP 0860882 A2	26-08-1998
		JP 10294325 A	04-11-1998
		TW 388942 B	01-05-2000